CLAIM LISTING

Although no claims are amended in this response, the following claim listing is provided for the Examiner's convenience:

1. **(Original)** A system for securely transmitting and storing data comprising:

a client arrangement which encrypts sensitive data using a first key to generate pre-encrypted sensitive data, the client encrypting non-sensitive data and the pre-encrypted sensitive data using a second key; and

a private network arrangement including:

a record database including a set of records,

a key-store database including a set of third keys which are encrypted using a fourth key,

a fuzzy signature database including signature vectors which are encrypted using the first key,

a permission database including authorization information, and

an application server locating one of the signature vectors in the fuzzy signature database which substantially corresponds to a query request, performing at least one relational database operation on an encrypted query request, and determining if a first user is authorized to perform an operation, using the authorization information,

wherein, if the first user is authorized, the application server obtains the fourth key for decrypting a particular key of the third keys which corresponds to particular information for a second user stored in the key-store database, and

wherein the application server decrypts the sensitive data obtained from the record database using the particular key.

2. **(Original)** The system of claim 1, further comprising:

a communication network arrangement connecting the private network arrangement to the client arrangement.

3. **(Original)** The system of claim 2, wherein the communication network arrangement is a public network arrangement.

4. **(Original)** The system of claim 3, further comprising:

an interface server connecting the public network arrangement to the private network arrangement.

5. **(Original)** The system of claim 4, further comprising:

a verification processor authenticating the interface server.

6. **(Original)** The system of claim 1, wherein the records include non-privileged user records and privileged user records.

7. **(Original)** The system of claim 1, wherein the first key is a public key of the first user.

8. **(Original)** The system of claim 1, wherein the second key is a public key of the application server.

9. **(Original)** The system of claim 1, wherein the third keys include private keys, each key corresponding to a separate user.

10. **(Original)** The system of claim 1, wherein the fourth key is a key-store master key which is utilized for accessing the key-store database.

11. **(Original)** A system for performing a secure transfer of client data, comprising:

a client arrangement which encrypts sensitive data using a first key to generate pre-encrypted sensitive data, the client arrangement encrypting non-sensitive data and the pre-encrypted sensitive data using a second key to generate the client data.

12. **(Original)** The system of claim 11, wherein the first key is a public key of a user.

13. **(Original)** The system of claim 11, wherein the second key is a public key of the application server.

14. **(Original)** A method for performing a secure transfer of client data, comprising the steps of:

encrypting sensitive data of the client data using a first key to generate pre-encrypted data; and

encrypting non-sensitive data of the client data and the pre-encrypted data using a second key.

15. **(Original)** The method of claim 14, wherein the first key is a public key of a user.

16. **(Original)** The method of claim 14, wherein the second key is a public key of an application server.

17-28. **(Withdrawn)**

29. **(Original)** A system for searching a record database which includes a plurality of records, each of the records including encrypted sensitive data, the system comprising:

an application server encrypting a search query which includes sensitive information using a key to generate an encrypted search query, and locating a particular record of the records in the record database if the sensitive information of the particular record substantially corresponds to the encrypted sensitive information of the encrypted search query.

30. **(Original)** The system of claim 29, wherein the record database stores non-privileged user records and privileged user records.

31. **(Original)** The system of claim 29, wherein the key is a public key of a user.

32. **(Original)** A method for searching a record database which includes a plurality of records, each of the records including encrypted sensitive data, the method comprising the steps of:

encrypting a search query which includes sensitive information using a key to generate an encrypted search query; and

locating a particular record of the records in the record database if the sensitive information of the particular record substantially corresponds to the encrypted sensitive information of the encrypted search query.

33. **(Original)** The method of claim 32, wherein the record database stores non-privileged user records and privileged user records.

34. **(Original)** The method of claim 32, wherein the key is a public key of a user.

35. **(Original)** A system for accessing encrypted sensitive data in a record database which includes a plurality of records, the system comprising:

a permission database including authorization information; and

an application server performing the following:

checking the permission data in the database to determine if a first user is authorized to perform a particular operation,

obtaining a first key if the first user is authorized to perform the particular operation,

obtaining a second key using the first key, decrypting the second key which corresponds to information for a second user, and

decrypting the encrypted sensitive data in the record database using the second key.

36. **(Original)** The system of claim 35, wherein the second key is located in a key-store database.

37. **(Original)** The system of claim 35, wherein the first key is a key-store master key.

38. **(Original)** The system of claim 35, wherein the second key is a private key of a user.

39. **(Original)** A method for accessing encrypted sensitive data in a record database which includes a plurality of records, comprising the steps of:

checking a permission data in the database to determine if a first user is authorized to perform a particular operation;

obtaining a first key if the first user is authorized to perform the particular operation,;

obtaining a second key using the first key, decrypting the second key which corresponds to information for a second user; and

decrypting the encrypted sensitive data in the record database using the second key.

40. **(Original)** The method of claim 39, wherein the second key is located in a key-store database.

41. **(Original)** The method of claim 40, wherein the first key is a key-store master key.

42. **(Original)** The method of claim 40, wherein the second key is a private key of a user.

43. **(Original)** A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions including particular instructions which, when executed by a processor connected to a communication network, cause the processor to perform the steps of:

encrypting sensitive data of a client data using a first key to generate pre-encrypted data; and

encrypting non-sensitive data of the client data and the pre-encrypted data using a second key.

44. **(Withdrawn)**

45. **(Original)** A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions including particular instructions which, when executed by a processor connected to a communication network, cause the processor to perform the steps of:

encrypting a search query which includes sensitive information using a key to generate an encrypted search query; and

locating a particular record of records in a record database if the sensitive information of the particular record substantially corresponds to the encrypted sensitive information of the encrypted search query.

46. **(Original)** A machine-readable medium having stored thereon data representing sequences of instructions, the sequences of instructions including particular instructions which, when executed by a processor connected to a communication network, cause the processor to perform the steps of:

checking a permission data in the database to determine if a first user is authorized to perform a particular operation;

obtaining a first key if the first user is authorized to perform the particular operation;

obtaining a second key using the first key, decrypting the second key which corresponds to information for a second user; and

decrypting the encrypted sensitive data in the record database using the second key.